Аннотация: В статье рассматриваются актуальные вопросы системной организации коммуникаций в направлении «власть – граждане» в пределах национальной территории Украины, в частности, в зоне вооруженного конфликта (Донбасс). Под термином «власть» подразумеваются исполнительные органы всех уровней национальной структуры государственного управления.

Ключевые слова: информационное пространство, информационная война, национальная идея, коммуникативные каналы, коммуникативные барьеры, убеждения, ожидания.

Abstract: The article is devoted to topical questions of systematic communication's organization in the direction «authority – citizens» on the territory of Ukraine, especially in the area of armed conflict (Donbas). The term of «authority» means executive organs of all levels of national structure of state management.

Key words: information space, information war, national idea, communication channel, barrier of perception, convictions, expectations.

УДК 351.86:004.056

КОЗЮРА Валерій Дмитрович
ХОРОШКО Володимир Олексійович
ШЕЛЕСТ Михайло Євгенійович

АНАЛІЗ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Постановка проблеми. Формування та розвиток сучасного інформаційного суспільства базується на синтезі двох технологій: комп'ютерної та телекомунікаційної й визначається двома простими, але дуже змістовними законами [1]: 1) Гордона Мура – «…кількість транзисторів у процесорах збільшуватиметься вдвічі кожних півтора роки…», який фактично пояснює виникнення нових специфічних за формою і способами суб'єктів і об'єктів інформаційної інфраструктури, а також гарантоване зростання швидкості обчислень і об'ємів оброблюваної інформації; 2) Роберта Меткалфа – «…цінність мережі знаходиться у квадратичній залежності від кількості вузлів, які є її складовими», тобто основу сучасного інформаційного суспільства становлять мережі різного функціонального призначення, а також новітні інформаційно-телекомунікаційні (ІТ) технології, які стали важливою складовою суспільного розвитку світової економіки в цілому й разом з тим значною мірою

змінили механізми функціонування суспільних інститутів та інститутів державної влади, а також увійшли до числа найбільших суттєвих факторів, які впливають на формування сучасного високоорганізованого інформаційного середовища.

Поступове поєднання інформаційно-телекомунікаційних систем (ІТС) і мережевих технологій, які в процесах обробки, передачі та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення призвело до формування кіберпростору – високорозвиненої моделі об'єктивної реальності, у якій відомості про особи, предмети, факти, події, явища і процеси подані у деякому математичному, символьному або будь-якому іншому виді, розміщуються в пам'яті фізичних пристроїв, перебувають у постійному русі за сукупністю ІТ систем і мереж.

Про важливість кіберпростору свідчить поява концепції ведення кібервоєн у ньому, створення у збройних силах деяких країн світу (США, Росія, Китай та інші) спеціальних структур, призначених для ведення такої боротьби і реалізуючих комплекс заходів, спрямованих на здійснення управлінського та/або деструктивного впливу власних інформаційних ресурсів шляхом використання спеціальних апаратно-програмних засобів [2].

Такий стан справ дає можливість говорити про наступні проблеми:

1) поява зовсім нових загроз безпеці як для об'єктів критично важливої інфраструктури держави, так і для громадян та суспільства в цілому. Це потребує переходу на вищий ступінь досліджень, спрямованих на всебічний аналіз методів, засобів, тактики та стратегії дій у кіберпросторі;

2) безпрецедентне розголошення персональних даних, важливих корпоративних ресурсів, конфіденційної інформації та інформації, що становить державну або іншу, передбачену законом, таємницю;

3) трансформація безпечного сектору держави за напрямами:

– пошуку і добування інформації шляхом вдосконалення способів й методів організації і проведення атак на ІТС, захищені криптосистеми протиборчих сторін та автоматизації усіх супутніх цьому процесів;

– обміну інформацією шляхом розробки принципово нових ІТС спеціального призначення;

– захисту власного інформаційного ресурсу від внутрішніх та зовнішніх кібервтручань та загроз.

Аналіз останніх досліджень і публікацій. Дослідженню проблем кібербезпеки держави останніми роками приділяється серйозна увага. З'явилася низка підручників, наукових статей [2; 5–10], які тією або іншою мірою розкривають сформульовані вище проблеми. Зокрема, в них висвітлено головні принципи забезпечення інформаційної та кібернетичної безпеки, розкрито їхню сутність, основний зміст та складові [1]; сформульовано поняття комп'ютерної злочинності та кібертероризму як загроз інформаційній та кібербезпеці, розглядається система державних органів забезпечення інформаційної безпеки України [3]; глибоко аналізуються питання інформаційній війни як форми ведення інформаційного протиборства [4].

Для розуміння серйозності проблеми, пов'язаної з кіберзагрозами, наводимо хронологію цільових кібератак, реалізованих в Україні за останні два роки:

– травень 2014 року – атака на ІТС ЦВК України;

– травень 2014 року – атака на підприємства транспортної сфери;

– серпень 2014 року – застосування трояна BlackEnergy – атака на широкий спектр органів влади України;

– жовтень 2015 року – застосування трояна BlackEnergy – атака на медіакомпанії, знищення відеоархівів, виведення із ладу робочих місць;

– грудень 2015 року – застосування трояна BlackEnergy – атака на деякі обленерго, виведення із ладу АСУ ТП підстанцій (30) і знеструмлення значного числа споживачів у західній Україні (близько 230 тисяч мешканців);

– січень 2016 року – спроба атаки на аеропорт «Бориспіль» за допомогою трояна BlackEnergy [9].

За даними М. Ярової, у 2015 році Україна стала абсолютним лідером за внутрішніми і зовнішніми кіберзагрозами в Європі [10].

Метою статті є аналіз сучасного стану кібербезпеки інформаційного суспільства в контексті забезпечення інформаційної безпеки держави. У відповідності з метою постає завдання упорядкування основних шляхів вдосконалення системи кібербезпеки України.

Виклад основного матеріалу. Глибинні зміни у ставленні більшості держав до власної інформації й, як наслідок, кібербезпеки (рис. 1), до стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі від стороннього впливу спричинили постановку завдань своєчасного виявлення, запобігання й нейтралізації реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним та державним інтересам [1; 3].

Із розвитком інформаційно-комунікаційних технологій (ІКТ), ІТС та глобальної мережі Інтернет світове суспільство, крім отриманих значних можливостей щодо обміну інформацією, стало надто уразливим від стороннього кібернетичного впливу, а саме від фактично неприхованих спроб впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної та спеціальної техніки з відповідним програмним забезпеченням [1; 5].

Інструктивні матеріали Інтернету поділяють кібервтручання або кіберзагрози на такі групи:

– власне комп'ютерні інциденти, що полягають у втручанні в роботу обчислювальних систем, порушенні авторських прав на програмне забезпечення, а також розкраданні даних і комп'ютерного часу тощо;

– інциденти, «пов'язані з комп'ютерними», що супроводжують головним чином протиправні дії за напрямом фінансового шахрайства;

– мережеві інциденти, що сприяють здійсненню незаконних угод [1].

Рис. 1 – Об'єкти впливу в інформаційному та кіберпросторах

Існує й інша класифікація таких дій, яка визначає сім основних груп, що можна віднести до способів або методів, використовуваних порушниками для здійснення нападу, а саме:

– перехоплення паролів користувачів;

– «соціальна інженерія»;

– використання помилок програмного забезпечення і програмних закладок;

– використання помилок механізмів ідентифікації користувачів;

– використання недосконалості протоколів передачі даних;

– одержання інформації про користувачів стандартними засобами операційних систем;

– блокування сервісних функцій системи, що атакується [5].

Найбільший інтерес з позицій класифікації кібернетичних втручань і загроз становить схема, яка запропонована Конвенцією Ради Європи по боротьбі з кіберзлочинністю. У ній говориться про чотири можливі групи таких дій [1].

Перша група це інциденти, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних даних і систем, що реалізуються через:

– несанкціонований доступ у інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або її частини, а також до інформаційних ресурсів протиборчої сторони, зроблений в обхід систем захисту);

– втручання в дані (протиправне змінювання, знешкодження, видалення, перекручування або блокування комп'ютерних даних та керуючих команд шляхом проведення кібератак на ІТС, ресурси та мережі державного та іншого управління);

– втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи шляхом роз-

робки та поширення шкідливого програмного забезпечення, застосування апаратних та програмних закладок, радіоелектронного та інших видів впливу на технічні засоби та системи телекомунікації, системи захисту інформаційних ресурсів, систем і мереж, програмно-математичного забезпечення, протоколи передачі даних, алгоритми адресації та маршрутизації тощо);

– незаконне перехоплення (протиправне навмисне перехоплення непризначених для загального доступу комп'ютерних даних, переданих мережами спеціального призначення в обхід заходів захисту та безпеки);

– незаконне використання комп'ютерного й телекомунікаційного устаткування (виготовлення, придбання для використання, поширення або інші способи зробити доступними дані: пристрої, виключаючи програмне забезпечення, розроблені або пристосовані для здійснення кожного зі злочинів першої групи; комп'ютерні паролі, коди доступу, інші подібні дані, що забезпечують доступ до комп'ютерної системи або її частини) або його повне вилучення.

Друга група – це шахрайство та підробка, пов'язані з використанням комп'ютерів, що полягають у:

– підробці документів із застосуванням комп'ютерних засобів (протиправне навмисне внесення змістовних спотворень, вилучення або блокування комп'ютерних даних, що позначається на вірогідності документів);

– шахрайстві із застосуванням комп'ютерних засобів (втручання у функціонування комп'ютерної системи з метою навмисного протиправного одержання економічної вигоди для себе або для інших осіб).

Третя група – це інциденти, пов'язані з розміщенням у мережах протиправної інформації.

Четверта група – це інциденти щодо авторських і суміжних прав.

Зазначені переліки не є вичерпними, але вони дають можливість, по-перше, умовно об'єднати вказані типи дій у дві укрупненні категорії – втручання та загрози, спрямовані безпосередньо на порушення нормального функціонування ІТС та підключених до них комп'ютерів (тип 1 – за схемою, запропонованою конвенцією Ради Європи), а також «традиційні» протиправні дії (типи 2, 3, 4 – за тією ж схемою), що пов'язані з комп'ютером або вчинені за його допомогою; по-друге, зробити висновок про те, що ці дії у кіберпросторі вийшли за межі окремих країн й набули при цьому істотної фінансової підтримки та якісних комунікацій; по-третє, формалізувати зазначені типи дій, зобразивши їх моделлю, яка міститиме три головні етапи:

– вивчення певного об'єкта;

– здійснення нападу на нього;

– приховування слідів нападу.

Крім того, в кожному етапі повинні бути стадії інформаційного обміну і нападу. Вони, у свою чергу, складаються з операцій щодо обміну даними, рекогносцировки, скасування й складання карти дій (характерні для інформаційного обміну), а також з операцій одержання доступу, розширення повноважень, крадіжки інформації, бомбування, знищення слідів, створення «чорних ходів» і відмови в обслуговуванні (характерні для здійснення нападу).

Останнім часом саме такі дії реалізовуються протиборчими сторонами з метою порушення або блокування роботи ІТС і мереж стратегічно важливих галузей (об'єктів) інфраструктури, в тому числі військового, транспортного, фінансового, промислового та енергетичного секторів, а також несанкціонованого отримання інформації з відносно відкритих і закритих баз даних (баз знань) державних, комерційних та інших установ, їх модифікації та/або повного знищення [9].

За даними Інтернету, темпи їх зростання з року в рік неодмінно збільшуються [5; 7; 8]. Це спричинило появу принципово нового розподілу терористичних дій в кібернетичному просторі, який отримав назву – кібертероризм (терористична діяльність, що провадиться у кіберпросторі або з його використанням). Директор Центру захисту національної інфраструктури ФБР США Рональд Дік у доповіді, яка була опублікована на сайті ФБР, так характеризує ситуацію, що склалась на сьогодні: «… у світі сформувалась нова форма тероризму – кібертероризм, який використовує комп'ютер та мережі зв'язку для руйнування частин національної інфраструктури та досягнення власних цілей» [1].

Директор ЦРУ Джордж Тенет, виступаючи з проблем світових загроз, заявив, що розповсюдження кібертероризму може з часом набути значно більших, ніж очікувалось, масштабів і стати реальною загрозою для національної безпеки будь-якої держави. За його твердженням, вже більшість терористичних угруповань для підтримки своєї протиправної діяльності використовують останні досягнення інформаційних технологій та комп'ютерного прогресу – комп'ютерні файли, електронну пошту і криптографію та стеганографію. Підтвердженням цьому є той факт, що на сьогодні в Інтернеті представлені своїми веб-сторінками абсолютно всі відомі терористичні групи. Вони видають власні матеріали щонайменше на 40 різних мовах та у своїй діяльності застосовують здебільшого такі прийоми, як:

– завдання збитків окремим елементам інформаційного та кіберпростору;

– руйнування апаратних засобів, мереж електроживлення та елементної бази сучасних ІТС, а також наведення завад через використання спеціальних програм, біологічних та хімічних засобів;

– крадіжка або знищення інформаційних, програмних і технічних ресурсів інформаційного та кіберпростору, що мають суспільну значимість, шляхом подолання їх систем захисту, впровадження вірусів та різного роду закладок;

– вплив на програмне забезпечення та інформацію з метою їхнього перекручування або модифікації;

– розкриття та загроза опублікування або саме опублікування закритої інформації про функціонування інформаційної інфраструктури держави, суспільно значимі військові інформаційні системи, коди шифрування та принципи роботи шифрувальних систем;

– захоплення каналів засобів масової інформації з метою поширення дезінформації, чуток, демон-

страції сили терористичної організації та оголошення нею своїх вимог;

– знищення або активне придушення ліній зв'язку, штучне перевантаження вузлів комутації;

– проведення інформаційних і психологічних операцій тощо [7].

Основним способом дій кібертерористів є проведення атак на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних та інші складові ІТ інфраструктури протилежної сторони. Це сприятиме їх поширенню до атакованої системи, придушенню засобів мережевого інформаційного обміну, здійсненню інших деструктивних впливів тощо.

Висновки. Таким чином, характерними ознаками, які нині уособлюють поняття кібербезпеки є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційних ресурсів і технологій, ІТС, та які спрямовані на досягнення і утримання потенційними протиборчими сторонами перемоги в протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної інфраструктури.

Останнім часом такі дії займають чітку позицію в геополітичній конкуренції переважної більшості країн світу, що, в свою чергу, зумовлює нові завдання їх службам безпеки та збройним силам й виводить на перше місце проблему інформаційного протиборства.

Список використаних джерел

1 Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підруч. / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа ; за заг. ред. д-ра тех. наук, професора В. Б. Толубка. – К. : ДУТ, 2015. – 288 с. [Електронний ресурс]. – Режим доступу : http://www.dut.ua/ru/lib/1/category/1311/view/1209.

2 Бурячок В. Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона. – 2011. – № 3. – С. 35–42.

3 Основи інформаційної безпеки держави : навч. посіб. / [кол. авторів ; за заг. ред. Є. Д. Скулиша]. – К. : Наук.-вид. центр НА СБ України, 2013. – 388 с.

4 Інформаційна безпека (соціально-правові аспекти) : підруч. / В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк та ін. ; за заг. ред. Є. Д. Скулиша. – К. : КНТ, 2010. – 776 с.

5 Хорошко В. А. Кибертерроризм и информационная безопасность / В. А. Хорошко, М. Е. Шелест // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2014. – Вип. 1(27). – С. 14–19.

6 Козюра В. Д. Методика оцінки рівня безпеки інформаційного простору / В. Д. Козюра, С. Ж. Піскун, В. О. Хорошко, Ю. Є. Хохлачова // Інформаційна безпека людини, суспільства, держави. – 2013. – № 1 (11). – С. 121–126.

7 Хорошко В. О. Особливості застосування сучасної інформаційної зброї / В. О. Хорошко, Т. І. Козел, О. О. Ярошенко // Правове, нормативне та метрологічне забезпечення систем захисту

інформації в Україні. – 2015. – Вип. 1(29). – С. 15–19.

8 Гриненко І. Структура кримінальних відносин у кіберпросторі / І. Гриненко, Д. Прокоф'єва-Янчиленко, Д. Гончаренко // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2013. – Вип. 1(25). – С. 16–21.

9 Худынцев Н. Н. Основные направления государственной политики в сфере киберзащиты: нормативные и организационные аспекты / Н. Н. Худынцев [Електронний ресурс]. – Режим доступу : http://www.rcc.org.ru/3_khudyntsev.ppt.

10 Ярова М. Кібербезпека в Україні: у 2015 році наша країна – «найгарячіша» точка Європи / [Електронний ресурс]. – Режим доступу : http://news.finance.ua/ua/news/-/363836/kiberbezpeka-v-ukrayini-u-2015-rotsi-nasha-krayina-najgaryachisha-tochka-yevropy.

Аннотация: В статье анализируются факторы, оказывающие существенное влияние на состояние кибербезопасности информационного общества, которое строится в современной Украине. Особое внимание уделено вопросам систематизации киберугроз на объекты критической информационной инфраструктуры.

Ключевые слова: киберпространство, кибербезопасность, информационная безопасность, киберугроза, кибератака, кибертерроризм, киберпреступность.

Abstract: This paper analyzes the factors that have a significant impact on the cyber security of the information society, which is built in modern Ukraine. Particular attention is paid to the systematization of cyber threats to critical information infrastructure objects.

Key words: cyberspace, cyber security, information security, cyber threat, cyber attack, cyber terrorism, cyber-crime.